SPYWOLF

Security Audit Report

Audit prepared for

MSNAI

Completed on

March 14, 2024

SPYWOLF.CO
@SPYWOLFNETWORK
@SPYWOLFNETWORK

KEY RESULTS

Cannot mint new tokens	Passed
Cannot pause trading (honeypot)	*
Cannot blacklist an address	Passed
Cannot raise taxes over 25%?	Not Passed
No proxy contract detected	Passed
Not required to enable trading	Passed
No hidden ownership	Passed
Cannot change the router	Passed
No cooldown feature found	Passed
Bot protection delay is lower than 5 blocks	Passed
Cannot set max tx amount below 0.05% of total supply	Passed
The contract cannot be self-destructed by owner	Passed

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

N/A = Not applicable for this type of contract

*Can turn into honeypot involuntarily by contract's internal logic, if this happens it can be avoided by disabling contract's auto swap settings

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

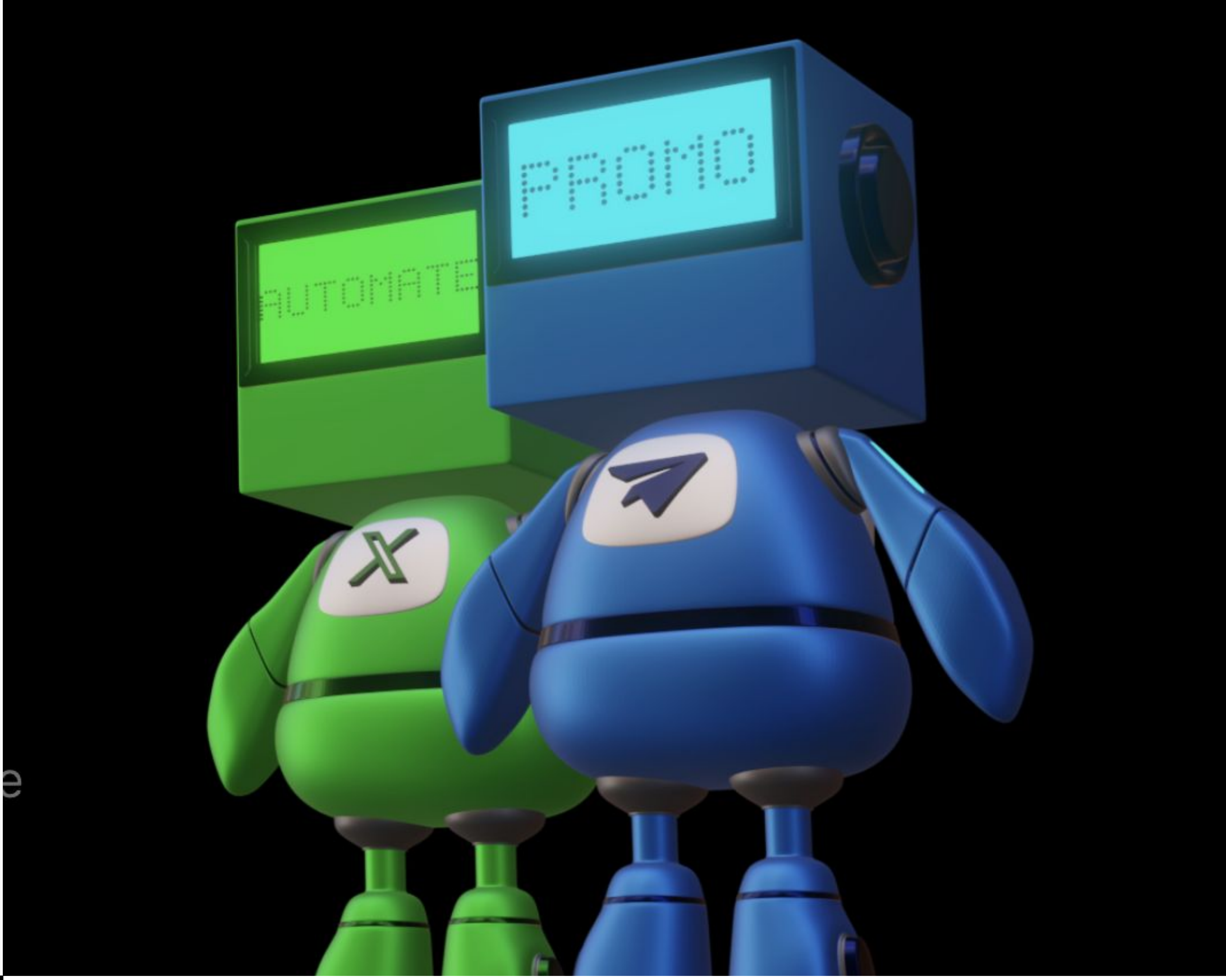
You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

MSNAI



PROJECT DESCRIPTION

According to their website:
$MSNAI streamlines promotional efforts to maximize marketing impact, reaching a wider audience as efficiently as possible. With AI assistance, developers and investors can grow exposure effortlessly across various social media platforms, enhancing visibility and engagement. Internal use of our bot allows for seamless scheduling, customization, and content creation to save time and resources. Moreover, personalized guided community engagement further boosts exposure and interaction, ultimately enhancing the project's success.

Release Date: Launching in March, 2024

Category: Utility token

CONTRACT INFO

Token Name
MSNAI

Symbol
MSNAI

Contract Address
0x457683C8C0DF1c16485c2274eA32703454cbE71B

Network
Ethereum

Language
Solidity

Deployment Date
March 14, 2024

Contract Type
Token with taxes

Total Supply
10,000,000

Status
Launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	359
Uniq Senders	32
Uniq Receivers	108
Total Amount	24730343.36204656 MSNAI
Median Transfer Amount	10116.581720929533 MSNAI
Average Transfer Amount	68886.7503121074 MSNAI
First transfer date	2024-03-14
Last transfer date	2024-03-14
Days token transferred	1

SMART CONTRACT STATS

Calls Count	819
External calls	82
Internal calls	737
Transactions count	234
Uniq Callers	87
Days contract called	1
Last transaction time	2024-03-14 23:33:59 UTC
Created	2024-03-14 19:19:35 UTC
Create TX	0xde996a99906d6b1f6dd98f68debc0ce695d3e9284de47b8541d12a36cca93fd4
Creator	0x1DBbBd6bE920bC21c7FdfbB250497b5bE6234D55

FEATURED WALLETS

Owner address	0x1DBbBd6bE920bC21c7FdfbB250497b5bE6234D55
Marketing fee receiver	0xc4aEB15b65B465136FD159A846B25aDdc9DB00dB
LP address	0x2A37331D8349CAEe9c6414C972231BF34FAb0a86 98.6% of total LP supply is locked in Unicrypt https://app.uncx.network/amm/uni-v2/pair/0x2a37331d8349caee9c6414c972231bf34fab0a86 Unlocks at 14/09/2024 21:51

TOP 3 UNLOCKED WALLETS

20%	Marketing wallet 0xc4aEB15b65B465136FD159A846B25aDdc9DB00dB
15%	Strategic wallet 0x6c66e5d4eB1f6891AD27c5832425D054765dcF76
5%	Development wallet 0x1DBbBd6bE920bC21c7FdfbB250497b5bE6234D55

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

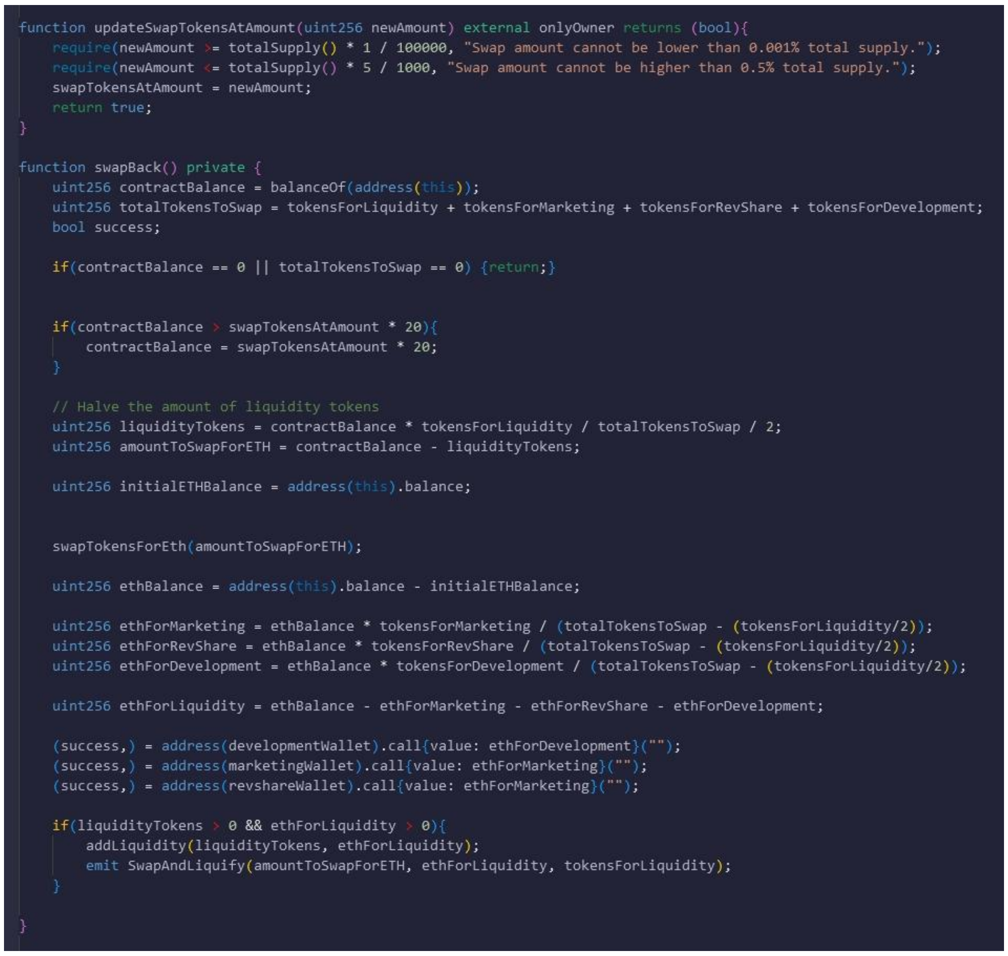
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

When swapTokensAtAmount is set to low number and autoSwap is enabled and enough tokens with bnb are accumulated in the contract, contract may halt on sell causing all sells to fail.
Marketing share is sent twice.



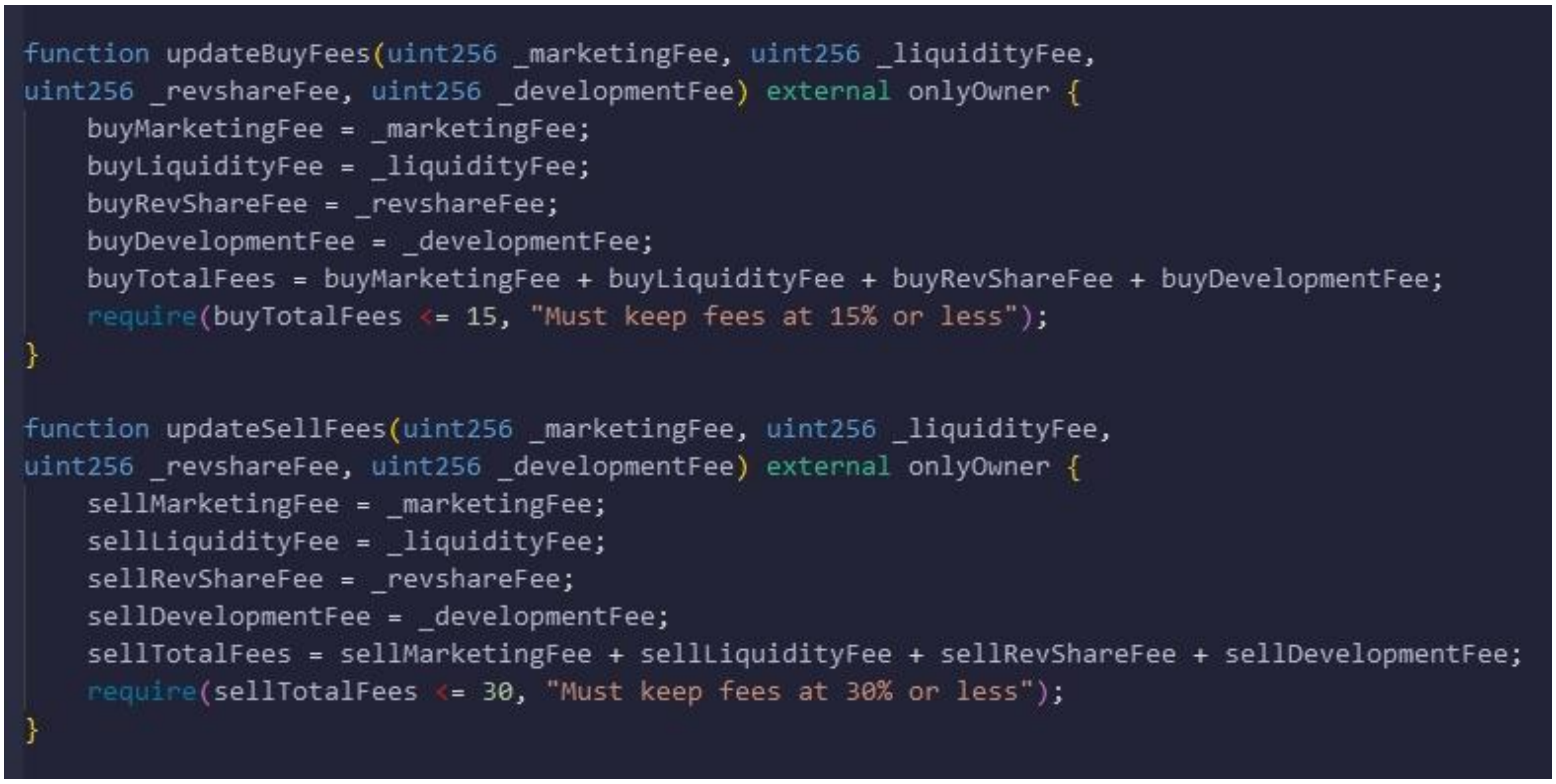
```
function updateSwapTokensAtAmount(uint256 newAmount) external onlyOwner returns (bool){
    require(newAmount >= totalSupply() * 1 / 100000, "Swap amount cannot be lower than 0.001% total supply.");
    require(newAmount <= totalSupply() * 5 / 1000, "Swap amount cannot be higher than 0.5% total supply.");
    swapTokensAtAmount = newAmount;
    return true;
}

function swapBack() private {
    uint256 contractBalance = balanceOf(address(this));
    uint256 totalTokensToSwap = tokensForLiquidity + tokensForMarketing + tokensForRevShare + tokensForDevelopment;
    bool success;

    if(contractBalance == 0 || totalTokensToSwap == 0) {return;}


    if(contractBalance > swapTokensAtAmount * 20){
        contractBalance = swapTokensAtAmount * 20;
    }

    // Halve the amount of liquidity tokens
    uint256 liquidityTokens = contractBalance * tokensForLiquidity / totalTokensToSwap / 2;
    uint256 amountToSwapForETH = contractBalance - liquidityTokens;

    uint256 initialETHBalance = address(this).balance;


    swapTokensForEth(amountToSwapForETH);

    uint256 ethBalance = address(this).balance - initialETHBalance;

    uint256 ethForMarketing = ethBalance * tokensForMarketing / (totalTokensToSwap - (tokensForLiquidity/2));
    uint256 ethForRevShare = ethBalance * tokensForRevShare / (totalTokensToSwap - (tokensForLiquidity/2));
    uint256 ethForDevelopment = ethBalance * tokensForDevelopment / (totalTokensToSwap - (tokensForLiquidity/2));

    uint256 ethForLiquidity = ethBalance - ethForMarketing - ethForRevShare - ethForDevelopment;

    (success,) = address(developmentWallet).call{value: ethForDevelopment}("");
    (success,) = address(marketingWallet).call{value: ethForMarketing}("");
    (success,) = address(revshareWallet).call{value: ethForMarketing}("");

    if(liquidityTokens > 0 && ethForLiquidity > 0){
        addLiquidity(liquidityTokens, ethForLiquidity);
        emit SwapAndLiquify(amountToSwapForETH, ethForLiquidity, tokensForLiquidity);
    }

}
```

- Recommendation:
  - ○ Consider more efficient formula for autoswap, auto liquidity and auto tokens distribution

FOUND THREATS

⚠ Medium Risk

Owner can set buy fees up to 15% and sell fees up to 30%.
Combined buy+sell = 45%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.



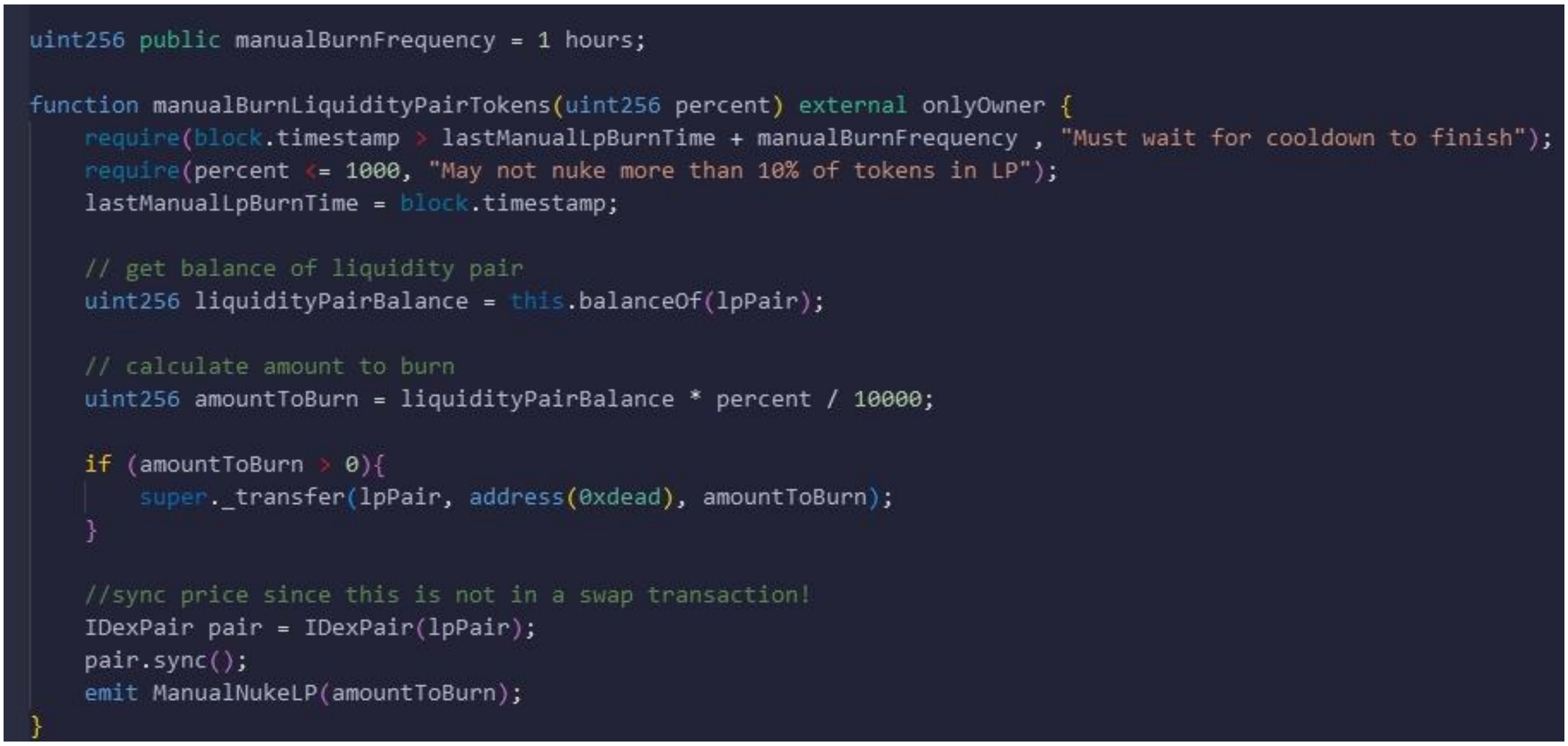
```
function updateBuyFees(uint256 _marketingFee, uint256 _liquidityFee,
uint256 _revshareFee, uint256 _developmentFee) external onlyOwner {
    buyMarketingFee = _marketingFee;
    buyLiquidityFee = _liquidityFee;
    buyRevShareFee = _revshareFee;
    buyDevelopmentFee = _developmentFee;
    buyTotalFees = buyMarketingFee + buyLiquidityFee + buyRevShareFee + buyDevelopmentFee;
    require(buyTotalFees <= 15, "Must keep fees at 15% or less");
}

function updateSellFees(uint256 _marketingFee, uint256 _liquidityFee,
uint256 _revshareFee, uint256 _developmentFee) external onlyOwner {
    sellMarketingFee = _marketingFee;
    sellLiquidityFee = _liquidityFee;
    sellRevShareFee = _revshareFee;
    sellDevelopmentFee = _developmentFee;
    sellTotalFees = sellMarketingFee + sellLiquidityFee + sellRevShareFee + sellDevelopmentFee;
    require(sellTotalFees <= 30, "Must keep fees at 30% or less");
}
```

- Recommendation:
    - Considered as good practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ Low Risk

Owner can manually burn tokens from the liquidity pair up to 10% of current liquidity pair per hour.
Burning tokens from the liquidity pair will cause the price for each token to increase.

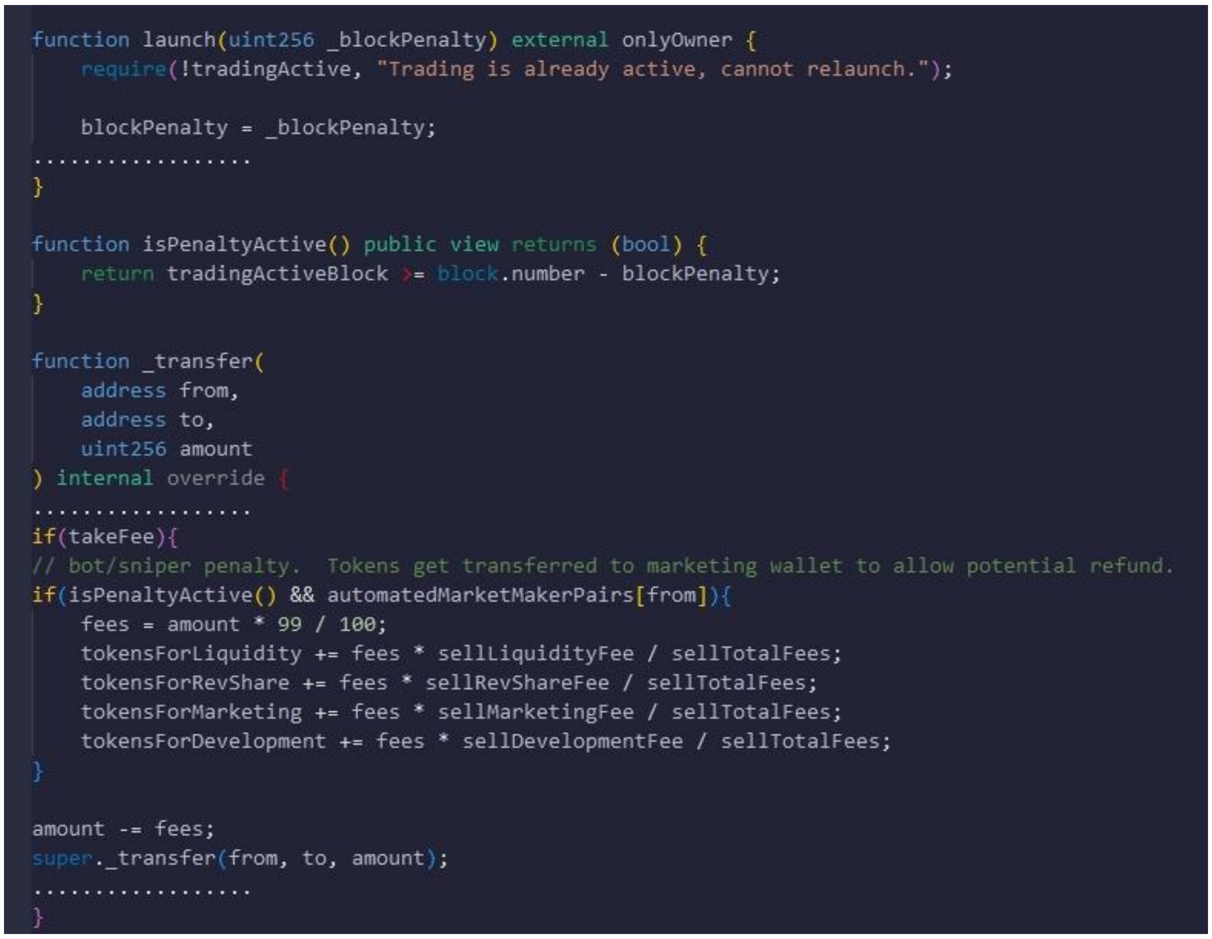


```
uint256 public manualBurnFrequency = 1 hours;

function manualBurnLiquidityPairTokens(uint256 percent) external onlyOwner {
    require(block.timestamp > lastManualLpBurnTime + manualBurnFrequency , "Must wait for cooldown to finish");
    require(percent <= 1000, "May not nuke more than 10% of tokens in LP");
    lastManualLpBurnTime = block.timestamp;

    // get balance of liquidity pair
    uint256 liquidityPairBalance = this.balanceOf(lpPair);

    // calculate amount to burn
    uint256 amountToBurn = liquidityPairBalance * percent / 10000;

    if (amountToBurn > 0){
        super._transfer(lpPair, address(0xdead), amountToBurn);
    }

    //sync price since this is not in a swap transaction!
    IDexPair pair = IDexPair(lpPair);
    pair.sync();
    emit ManualNukeLP(amountToBurn);
}
```

FOUND THREATS

Informational

Owner can initiate the launch function once.
Owner can set _blockPenalty without limitations.
Addresses which buy during the blockPenalty period will be subject to 99% fees. Token is already launched.



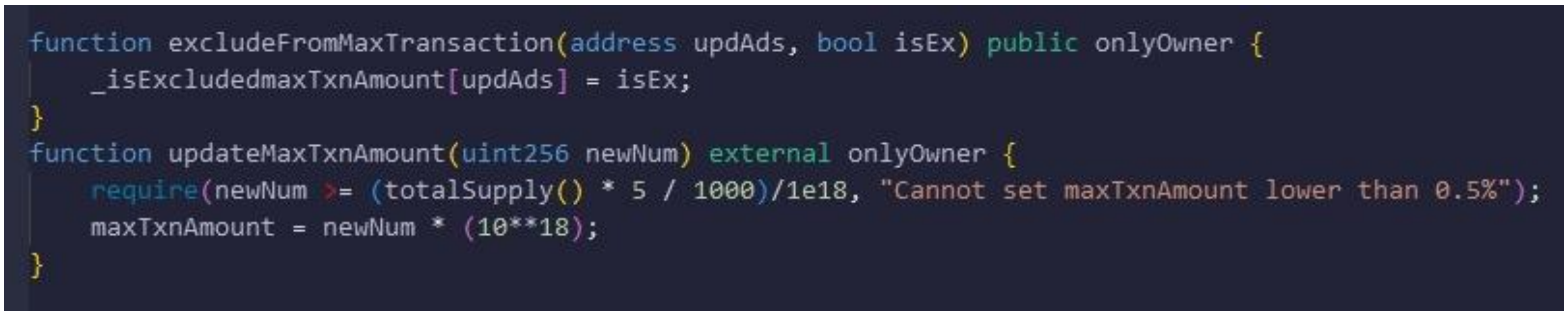
```
function launch(uint256 _blockPenalty) external onlyOwner {
    require(!tradingActive, "Trading is already active, cannot relaunch.");

    blockPenalty = _blockPenalty;
..................
}

function isPenaltyActive() public view returns (bool) {
    return tradingActiveBlock >= block.number - blockPenalty;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
..................
if(takeFee){
// bot/sniper penalty.  Tokens get transferred to marketing wallet to allow potential refund.
if(isPenaltyActive() && automatedMarketMakerPairs[from]){
    fees = amount * 99 / 100;
    tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
    tokensForRevShare += fees * sellRevShareFee / sellTotalFees;
    tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
    tokensForDevelopment += fees * sellDevelopmentFee / sellTotalFees;
}

amount -= fees;
super._transfer(from, to, amount);
..................
}
```

- Recommendation:
  - Considered as good practice is automated anti bot system to be up to 5 blocks after the initial trade start.
    Consider reasonable value for early penalty blocks.

FOUND THREATS

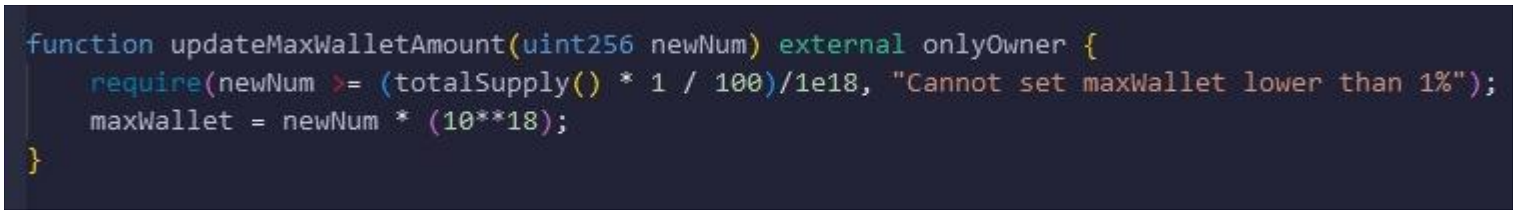
Informational

Owner can set max transaction limit but cannot lower it than 0.5% of total supply.
Owner can exclude address from max transaction and max wallet limit.



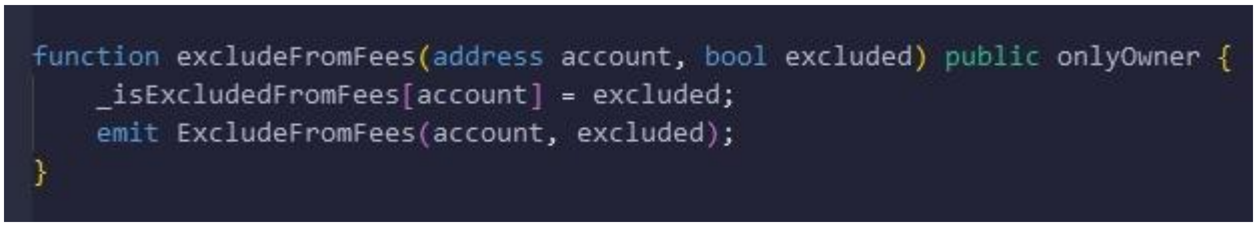
```
function excludeFromMaxTransaction(address updAds, bool isEx) public onlyOwner {
    _isExcludedmaxTxnAmount[updAds] = isEx;
}
function updateMaxTxnAmount(uint256 newNum) external onlyOwner {
    require(newNum >= (totalSupply() * 5 / 1000)/1e18, "Cannot set maxTxnAmount lower than 0.5%");
    maxTxnAmount = newNum * (10**18);
}
```

Owner can set max wallet limit but cannot lower it than 1% of total supply.



```
function updateMaxWalletAmount(uint256 newNum) external onlyOwner {
    require(newNum >= (totalSupply() * 1 / 100)/1e18, "Cannot set maxWallet lower than 1%");
    maxWallet = newNum * (10**18);
}
```

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

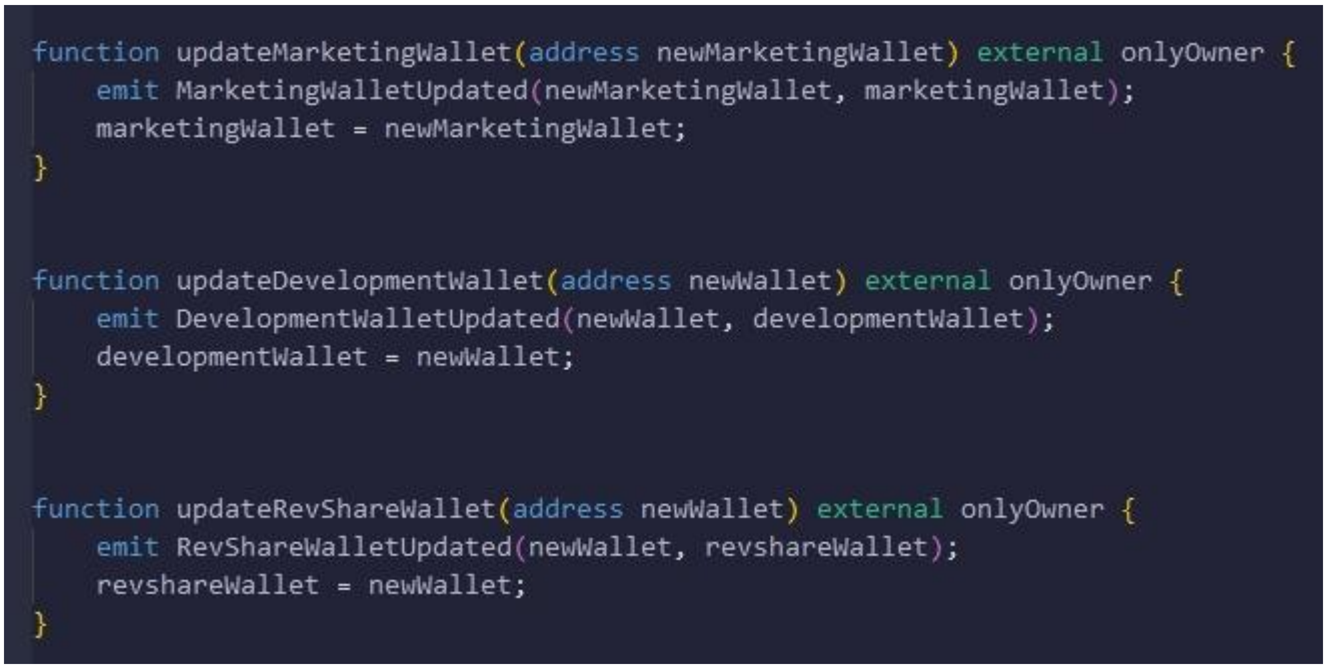


```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

FOUND THREATS

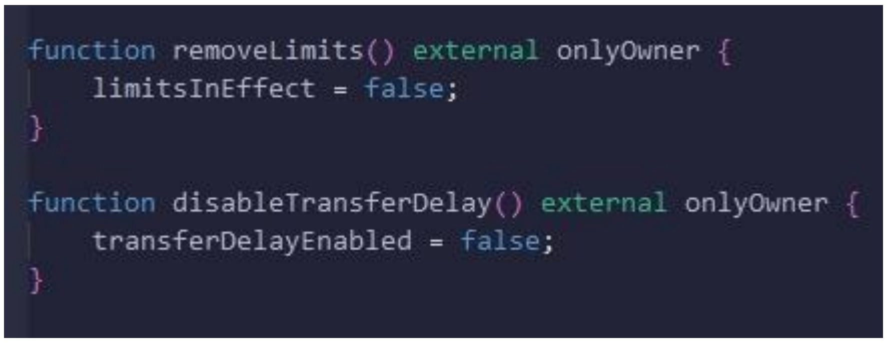
Informational

Owner can change marketing, development and revshare addresses.



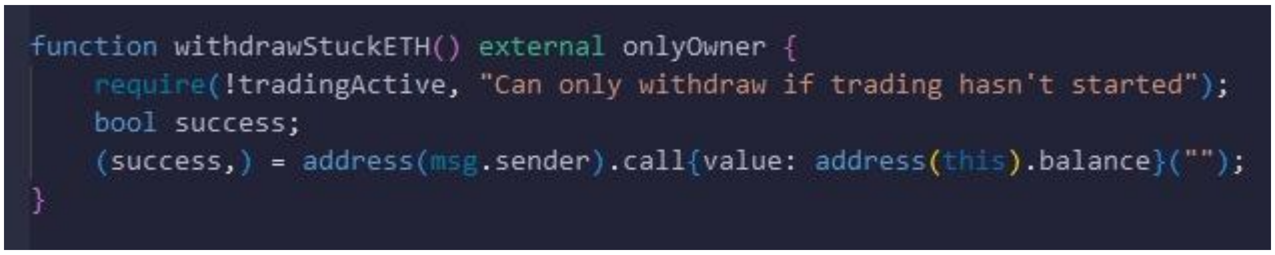
```
function updateMarketingWallet(address newMarketingWallet) external onlyOwner {
    emit MarketingWalletUpdated(newMarketingWallet, marketingWallet);
    marketingWallet = newMarketingWallet;
}


function updateDevelopmentWallet(address newWallet) external onlyOwner {
    emit DevelopmentWalletUpdated(newWallet, developmentWallet);
    developmentWallet = newWallet;
}


function updateRevShareWallet(address newWallet) external onlyOwner {
    emit RevShareWalletUpdated(newWallet, revshareWallet);
    revshareWallet = newWallet;
}
```

Owner can remove limits and transfer delay once.
Once removed, limits and transferdelay cannot be applied again.



```
function removeLimits() external onlyOwner {
    limitsInEffect = false;
}

function disableTransferDelay() external onlyOwner {
    transferDelayEnabled = false;
}
```

Owner can withdraw ETH from the contract only before token's launch function is initiated.

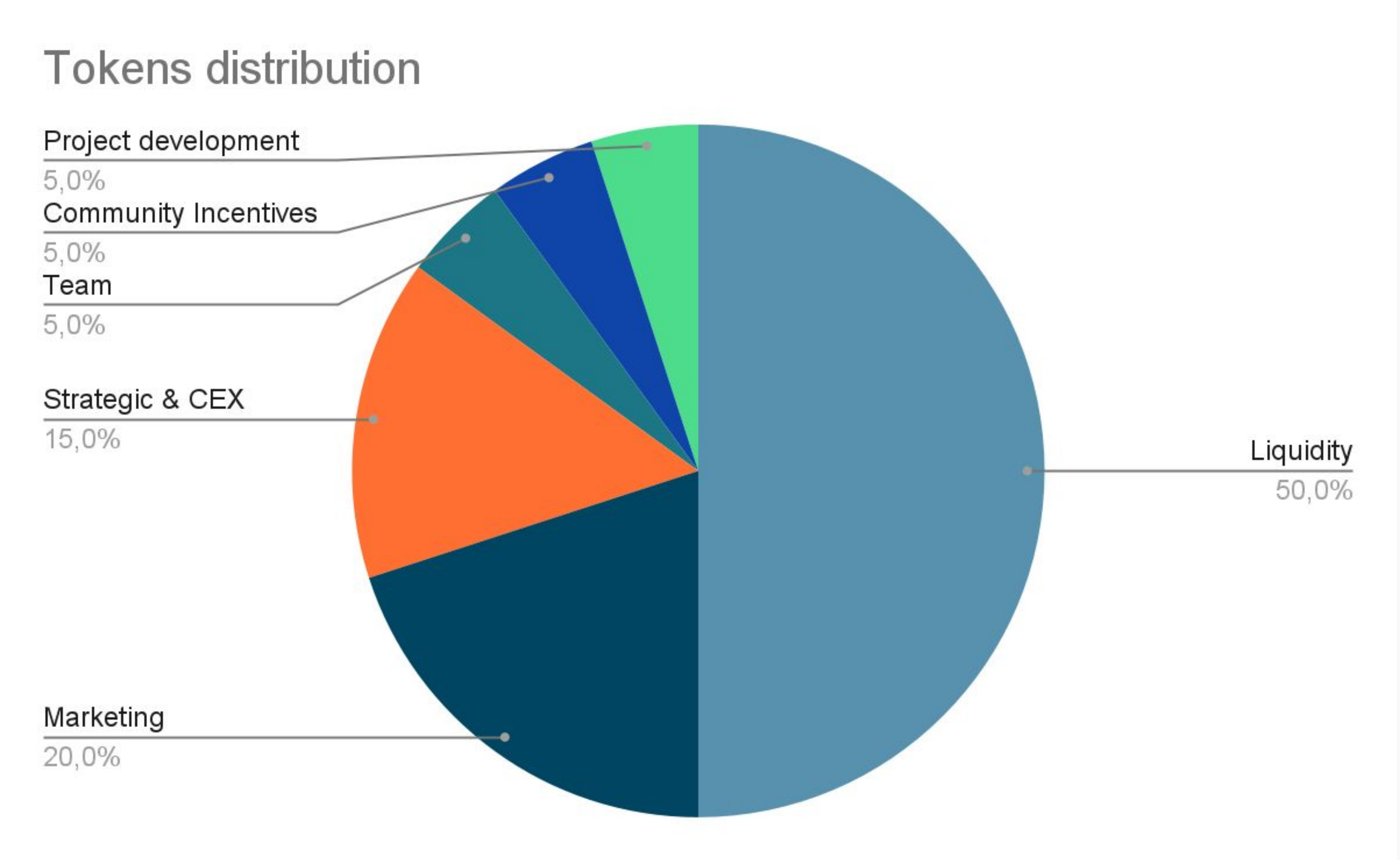


```
function withdrawStuckETH() external onlyOwner {
    require(!tradingActive, "Can only withdraw if trading hasn't started");
    bool success;
    (success,) = address(msg.sender).call{value: address(this).balance}("");
}
```

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 50% - Liquidity
- 20% - Marketing
- 15% - Strategic & CEX
- 5% - Project development
- 5% - Community incentives
- 5% - Team



WEBSITE

Website URL
https://msnai.bot/

Domain Registry
https://www.namecheap.com

Domain Expiration
2025-03-01

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

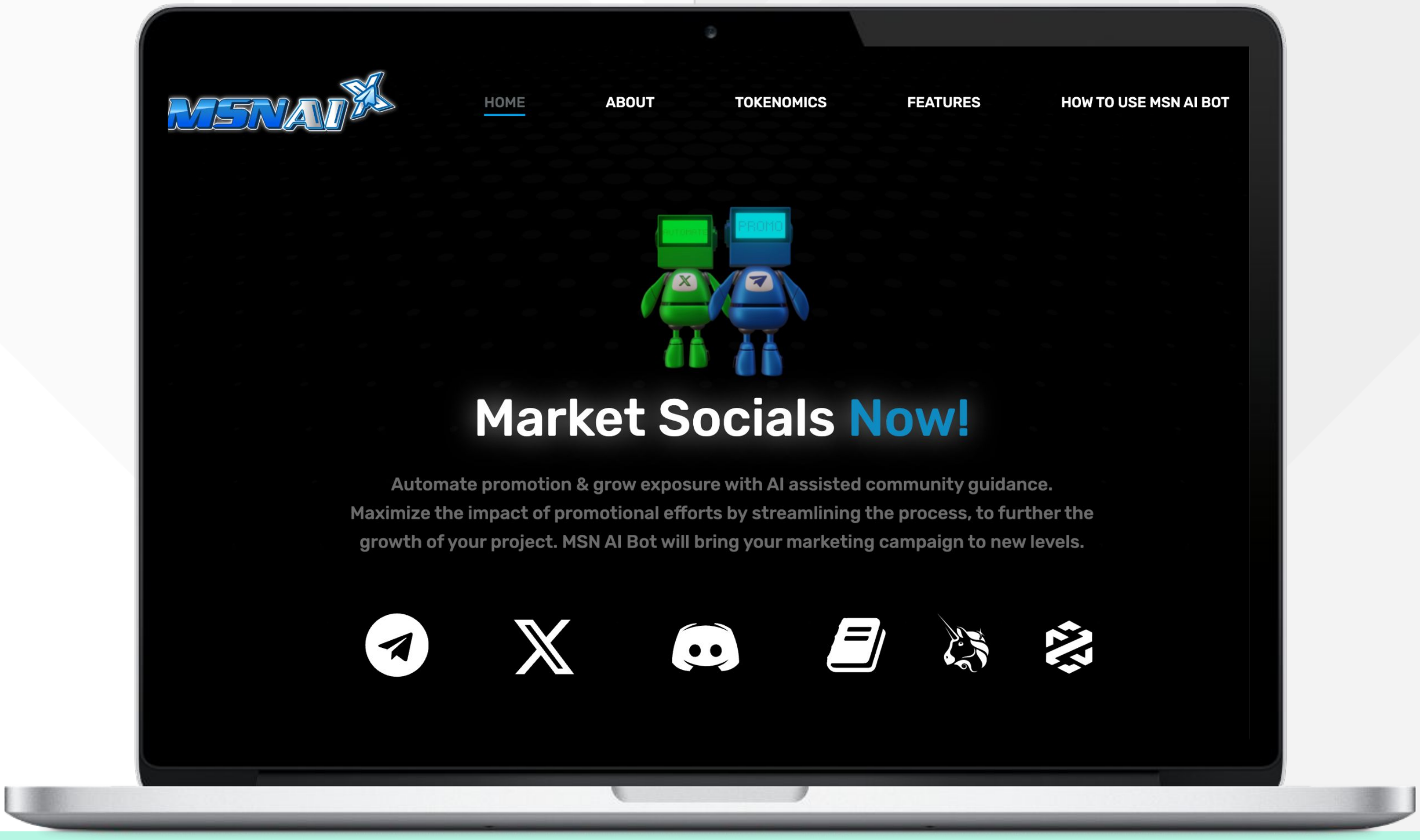
Design
Very nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes

Mobile-friendly?
Yes



Market Socials Now!

Automate promotion & grow exposure with AI assisted community guidance. Maximize the impact of promotional efforts by streamlining the process, to further the growth of your project. MSN AI Bot will bring your marketing campaign to new levels.

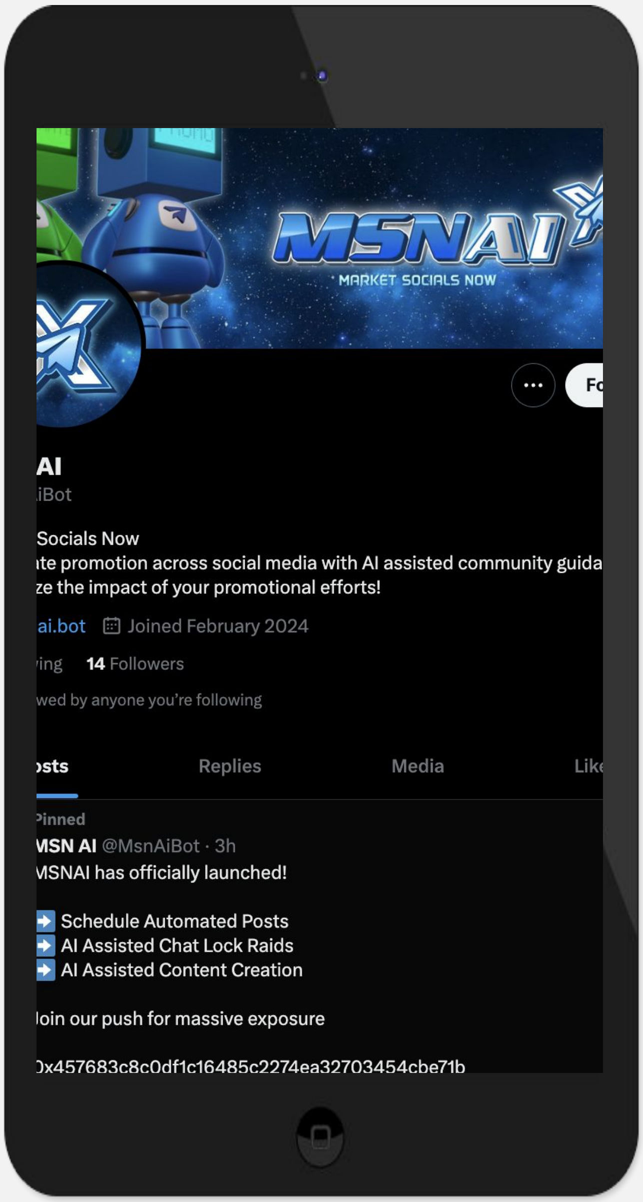
msnai.bot

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project’s social media pages are active



AI
iBot

Socials Now
ite promotion across social media with AI assisted community guida
ze the impact of your promotional efforts!

ai.bot Joined February 2024

ving **14** Followers

wed by anyone you’re following

osts Replies Media Like

Pinned
MSN AI @MsnAiBot · 3h
MSNAI has officially launched!

➡️ Schedule Automated Posts
➡️ AI Assisted Chat Lock Raids
➡️ AI Assisted Content Creation

Join our push for massive exposure

0x457683c8c0df1c16485c2274ea32703454cbe71b

Twitter's X

@MsnAiBot

- 6 followers
- 1 post total
- New account

Discord

https://discord.com/invite/VT7FMHkG

- 11 members
- Active members

Telegram

@MsnAiBotPortal

- 98 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.